IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

SKY FEDERAL CREDIT UNION and UNIVERSITY OF LOUISIANA FEDERAL CREDIT UNION, individually and on behalf of a class of all similarly situated financial institutions, and MD/DC CREDIT UNION ASSOCIATION, as an association on behalf of its members, Plaintiffs, v. EQUIFAX INC. Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Sky Federal Credit Union, University of Louisiana Federal Credit Union, and MD/DC Credit Union Association ("Plaintiffs") by their undersigned counsel, upon personal knowledge as to themselves and their own acts, and upon information and belief as to all other matters, bring this putative class action against Equifax Inc. ("Equifax" or "Defendant"), and allege as follows:

INTRODUCTION

1. Financial Institution Plaintiffs Sky Federal Credit Union and University of Louisiana Federal Credit Union ("FI Plaintiffs"), individually and on behalf of similarly situated banks, credit unions, and other financial institutions (the "Class" (defined below)), and MD/DC Credit Union Association ("Association Plaintiff"), acting on behalf of its members, bring this class action on behalf of financial institutions that suffered, and continue to suffer, financial losses and increased data security risks that are a direct result of Equifax's egregious failure to safeguard the financial institutions' customers' highly sensitive, personally identifiable information, including, but not limited to, names, Social Security numbers, birth dates, addresses, and driver's license numbers ("PII") and payment card data, including, but not limited to, credit and debit card numbers, primary account numbers ("PANs"), card verification value numbers ("CVVs"), expiration dates and zip codes ("Payment Card Data").

2. Specifically, between at least May 2017 and July 2017, Equifax was subject to one of the largest data breaches in this country's history when intruders gained access to the highly sensitive PII of over 145.5 million U.S. consumers – roughly 44% of the United States population – as well as the Payment Card Data for an untold number of credit and debit cards. Despite the fact that the threat of a data

breach has been a well-known risk to Equifax, as it acknowledged in its corporate filings, Equifax failed to take reasonable steps to adequately protect and affirmatively mishandled the only product in which it exclusively trades and is responsible for protecting: the ultra-sensitive, highly-sought-after personal and financial information of millions of individuals. Plaintiffs and the Class are now left to deal with the direct consequences of Equifax's failures and active misfeasance.

3. Equifax's CEO admitted: "The company failed to prevent sensitive information from falling into the hands of wrongdoers. . . . [T]he breach occurred because of both human error and technology failures."[1]

4. The data breach was the inevitable result of Equifax's longstanding approach to the security of consumers' confidential data, an approach characterized by its actions, neglect, incompetence, and an overarching desire to minimize costs.

5. Equifax's data security deficiencies were so significant that, even after hackers entered its systems, their activities went undetected for at least two months,

[1] Oversight of the Equifax Data Breach: Answers for Consumers: Hearing before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection (Oct. 3, 2017) (Prepared Testimony of Richard F. Smith), https://democrats-energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-the-equifax-data-breach-answers-for-consumers ("Smith Testimony").

despite red flags that should have caused Equifax to discover their presence and thwart, or at least minimize, the damage.

6. Equifax's actions left highly sensitive PII and Payment Card Data exposed and accessible to hackers for months. Consequently, the FI Plaintiffs have incurred and will continue to incur significant damages in cancelling and replacing customers' payment cards, covering fraudulent purchases, closing fraudulent bank and credit accounts, responding to credit disputes, taking protective measures to reduce risk of identity theft and loan fraud, and assuming financial responsibility for various types of fraudulent activity related to stolen identities and misuse of PII and Payment Card Data, among other things.

7. The financial harms caused by Equifax's negligent handling of PII and Payment Card Data have been, and will be, borne in large part by the financial institutions that issue payment cards, process and hold various loans and credit products, process and hold various deposit accounts, and service accounts that are held by individuals whose PII and Payment Card Data has been compromised by the breach. These costs include, but are not limited to, canceling and reissuing an untold number of compromised credit and debit cards, reimbursing customers for fraudulent charges, closing fraudulent bank and credit accounts, responding to credit disputes resulting from fraudulent accounts being opened as a result of compromised

customer data, increasing fraudulent activity, including the implementation of alternative customer authentication methods, monitoring, taking appropriate action to mitigate the risk of identity theft and fraudulent loans and other banking activity, sustaining reputational harm, and notifying customers of potential fraudulent activity.

8. FI Plaintiffs seek to recover the costs that they and others similarly situated have been forced to bear as a direct result of the Equifax data breach. Furthermore, FI Plaintiffs seek to obtain appropriate equitable relief to mitigate future harm that is certain to occur in light of the unprecedented scope of this breach.

PARTIES

FI Plaintiffs

9. Plaintiff Sky Federal Credit Union is a federally-chartered credit union with a principal place of business in Livingston, Montana.

10. Plaintiff University of Louisiana Federal Credit Union is a federally-chartered credit union with a principal place of business in Lafayette, Louisiana.

Association Plaintiff

11. Plaintiff MD/DC Credit Union Association ("MD/DC CUA") is a Maryland not-for-profit corporation and association for credit unions that operate in Maryland and Washington, D.C. whose members are financial institutions. MD/DC

CUA brings this action as an association on behalf of its members. MD/DC CUA has standing to assert its claims pursuant to established Supreme Court precedent. *United Food & Commer. Workers Union Local 751 v. Brown Group, Inc*., 517 U.S. 544, 553 (1996). MD/DC CUA has standing to bring this suit on behalf of its members because: (a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to MD/DC CUA's respective purposes; and (c) the injunctive relief sought does not require participation of MD/DC CUA's members.

12. The Association Plaintiff is an association whose members were damaged as a result of the data breach and likely will suffer further damage if another data breach occurs. The Association Plaintiff is a non-class plaintiff. While the Association Plaintiff has itself been injured by the data breach, it does not seek money damages. Rather, the Association Plaintiff brings this action for equitable relief on behalf of its members. The Association Plaintiff is as follows:

13. The Association Plaintiff is duly authorized to bring this action against Equifax. Many of the Association Plaintiff's members do not have the time or resources to pursue this litigation and fear retribution if they become named plaintiffs. Equifax has caused the Association Plaintiff to expend its own resources

assisting members injured by Equifax's data breach, and it has otherwise been directly and adversely impacted.

Defendant

14. Defendant Equifax Inc. is a publicly traded corporation with its principal place of business at 1550 Peachtree Street NE, Atlanta, Georgia.

JURISDICTION AND VENUE

15. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d). The aggregated claims of the individual class members exceed the sum or value of $5,000,000 exclusive of interest and costs; there are more than 100 putative class members defined below; and minimal diversity exists because the majority of putative class members are citizens of a different state than Defendant.

16. This Court has personal jurisdiction over Defendant because it maintains its principal headquarters in Georgia, is registered to conduct business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant intentionally avails itself of this jurisdiction by conducting its corporate operations here and promoting, selling, and marketing Equifax products and services to resident Georgia consumers and entities.

17. Venue is proper in this District under 28 U.S.C. §1391(a) because Equifax's principal place of business is in Georgia, and a substantial part of the events, acts, and omissions giving rise to the claims of the Plaintiffs occurred in this District.

FACTUAL ALLEGATIONS

Background

18. Equifax is the oldest and second-largest consumer credit reporting agency in the United States. Equifax was founded in 1899 and had $3.1 billion in revenue in 2016. Its common stock is traded on the New York Stock Exchange under the ticker symbol "EFX."

19. Equifax's 2016 Form 10-K states that it "is a leading global provider of information solutions and human resources business process outsourcing services for businesses, governments and consumers. We have a large and diversified group of clients, including financial institutions, corporations, governments and individuals. Our products and services are based on comprehensive databases of consumer and business information derived from numerous sources, including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data. We use advanced statistical techniques

and proprietary software tools to analyze all available data, creating customized insights, decision-making solutions and processing services for our clients."[2]

20. Equifax gathers and maintains credit-reporting information on over 820 million individual consumers and over 91 million businesses. Equifax gets its data from companies that have extended credit to consumers in the past, currently extend credit to consumers, or who wish to extend credit to consumers. Credit card companies, banks, credit unions, retailers, and auto and mortgage lenders all report the details of consumer credit activity to Equifax.[3]

21. In addition, Equifax obtains PII and Payment Card Data directly from consumers who purchase credit reporting, monitoring, and other products from Equifax. Equifax collects a substantial and diverse amount of sensitive personal information about consumers, including individuals' names, current and past addresses, birth dates, social security numbers, and telephone numbers; credit account information, including the institution name, type of account held, date an account was opened, payment history, credit limit, and balance; credit inquiry

---

[2] https://investor.equifax.com/~/media/Files/E/Equifax-IR/documents/financial-information/form-10-k.pdf (last accessed Oct. 3, 2017).

[3] *How Do Credit Reporting Agencies Get Their Information?* (July 2, 2014), https://blog.equifax.com/credit/how-do-credit-reporting-agencies-get-their-information/.

information, including credit applications; and public-record information, including liens, judgments, and bankruptcy filings.

22. Armed with this data, Equifax analyzes the information that it collects and sells four primary data products: credit services, decision analytics, marketing, and consumer assistance services:

a. **Credit Services.** Equifax generates consumer credit reports. When lending institutions, such as FI Plaintiffs, review a request for credit, they purchase a consumer credit report from Equifax to assist in making decisions about whether credit should be extended and in what amount.

b. **Decision Analytics.** Equifax also packages detailed transaction histories with analytics about the ways an individual interacts with certain debt. Credit issuers pay more for these reports, as they offer a deeper analysis of the appropriateness of certain credit for certain consumers.

c. **Marketing**. Credit issuers that offer pre-approved credit pay a marketing fee to Equifax for a list of consumers who meet predetermined requirements. This information is used to extend

offers of credit to consumers who meet an institution's desired criteria.

d. **Consumer Services.** Equifax also provides services directly to consumers, including credit monitoring and identity-theft-protection products. Additionally, Equifax is required by law to provide one free annual credit report to consumers.

23. Much like a bailment of personal property, the receipt by Equifax of uniquely-identifying consumer credit-reporting information, PII, and Payment Card Data, for Equifax's own business purposes places Equifax in a special relationship with the consumers, FI Plaintiffs, and the Class members, which rely on Equifax to maintain the security (and hence, the uniquely-identifying nature) of such information. The resulting harm to FI Plaintiffs and the Class members from mishandling the security and confidentiality of this information was, at all times, foreseeable to Equifax.

24. Equifax has a well-established and clear legal duty to act reasonably to protect the sensitive information that it collects and possesses from exposure to hackers and identity thieves.[4]

FI Plaintiffs Relied on Equifax to Adequately Protect Customers' Sensitive Information

[4] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. §1681(a)(4) and (b).

25. When FI Plaintiffs and Class members provide Equifax with their customers' most sensitive information, or when Equifax comes by such information in some other manner, FI Plaintiffs reasonably expect that such information will be stored by Equifax in a safe and confidential manner, using all reasonable safeguards and protections. The potential harm from doing otherwise is obvious to Equifax, which knows that FI Plaintiffs, as payment card issuers, lenders, and deposit account holders, bear the ultimate responsibility for identity theft and fraudulent lending and other consumer transactions.

26. Generally, financial institutions like FI Plaintiffs report to the credit reporting bureaus, including Equifax, on a monthly basis. FI Plaintiffs provide this confidential information to Equifax so that Equifax may use its expertise to aggregate, process, and analyze the information, so it can then be marketed to the financial services industry and to consumers directly. For example, financial institutions, like FI Plaintiffs, purchase the aggregated information from Equifax for purposes of analyzing the creditworthiness and financial condition of consumers. Equifax had a duty to properly secure its IT systems and website from hackers, to use available technology to encrypt and otherwise secure consumers' personal information using industry standard methods, and to act reasonably to prevent the

foreseeable harm to Plaintiffs and the Class, which it reasonably should have known would result from a data breach.

27. Indeed, Equifax's role as a credit-reporting firm made the need for it to secure the information it held especially acute. And that role has itself created an additional burden for financial institutions, which typically rely on the files at credit-reporting agencies, such as Equifax, to determine whether applications for consumer credit or loans are creditworthy. Not only has that process now been thrown into jeopardy for FI Plaintiffs and the Class they seek to represent, but also such financial institutions are now without a reliable, vital source of verifying consumers' identities due to the extent of the personal and financial information compromised by the Equifax breach.[5] The dire consequences of the increased risk of identity theft caused by Equifax's failures cannot be overemphasized. With the information used to establish a legal identity now available to identity thieves for over 145 million consumers, financial institutions are at a greatly increased risk of loan and deposit account fraud and payment card transaction fraud, and are left to devise and implement, and pay for, their own prophylactic measures to reduce such risk.

[5] *See* Telis Demos, *Equifax Hack Could Slow Down Fast Loans*, WALL STREET JOURNAL, Sept. 11, 2017, https://www.wsj.com/articles/equifax-hack-could-slow-down-fast-loans-1505147969.

28. For all of these reasons, the breach has sent shockwaves throughout the entire financial services industry, and its reverberations will be felt for years to come, each of which will inflict injury and damages on financial institutions, such as Plaintiffs and the Class.

The Equifax Data Breach

29. On September 7, 2017, Equifax announced a data breach event estimated to affect approximately 143 million U.S. consumers.

30. From at least May 13, 2017 to July 30, 2017, hackers exploited a vulnerability in Equifax's U.S. web server software to illegally gain access to certain consumer files. The attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.[6]

31. The potential vulnerability of the Apache Strut software was no secret. Numerous entities identified and issued public warnings in March 2017 regarding

---

[6] Equifax, *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes* (Sept. 15, 2017), https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/.

The alleged May 13, 2017 start date is based on Equifax's public statements of the results of its own investigation. Other sources, including Visa and MasterCard, have suggested that the breach may have started much earlier, as far back as November 2016.

the vulnerability, including The Apache Foundation, the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST"), and the U.S. Department of Homeland Security's Computer Emergency Readiness Team ("U.S. CERT"). Apache and NIST described the flaw as "critical," which is the highest rating those groups use to indicate the danger of a vulnerability. In the days that followed, media reports noted that hackers were already exploiting the vulnerability against various companies and government agencies.[7] Equifax has publicly stated that its security team "was aware of this vulnerability at that time [in March 2017]."[8]

32. On March 7, 2017, the same day the vulnerability was publicly announced, The Apache Foundation made available various patches and workarounds to protect against the vulnerability.[9] Despite this, Equifax affirmatively and actively continued to use the outdated version of the software for

---

[7] Dan Goodin, *Critical vulnerability under "massive" attack imperils high-impact sites*, ARSTECHNICA (Mar. 9, 2017), https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/.

[8] *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* note 6.

[9] Elizabeth Weise and Nathan Borney, *Equifax Had Patch 2 Months Before Hack and Didn't Install It, Security Group Says*, USA TODAY (Sept. 14, 2017), https://www.usatoday.com/story/money/2017/09/14/equifax-identity-theft-hackers-apache-struts/665100001/.

two and a half months without properly applying the available patches or taking other measures to protect against the flaw.[10] Equifax's conduct in this regard constitutes active misfeasance.

33. Specifically, on March 8, 2017, U.S. CERT sent Equifax a notice of the need to patch a particular vulnerability in the "Apache Struts" software used for its online disputes portal, where consumers can dispute items on their credit report.[11]

34. Equifax admitted that although it disseminated the U.S. CERT notification on March 9, 2017, and requested that the Apache Struts software be patched, the Equifax security department did not patch the software in response to the March 9, 2017 notification. *Id*. Equifax further admits that it was this unpatched vulnerability in the Apache Struts software that allowed hackers to access PII.

35. Over the multi-month period of the Equifax Data Breach, hackers accessed sensitive consumer information, including names, social security numbers, birth dates, addresses, and driver's license numbers. The compromised data contains complete profiles of consumers whose personal information was collected and maintained by Equifax.

---

10 *Id.*

11 Smith Testimony at 2-3, *supra* note 1.

36. In addition to accessing sensitive personal information, the hackers also accessed what Equifax purports to be 209,000 consumer credit card numbers, and an estimated 182,000 dispute records containing additional personal information.[12] Equifax stated that it believes all consumer credit card numbers were accessed in one fell swoop in mid-May 2017.

37. The hackers were also able to access Equifax's back-end servers, which are connected to financial institutions and enable the parties to share information digitally.[13] Such an intrusion has left credit issuers, including FI Plaintiffs, woefully exposed to the threat of hackers piggybacking off of Equifax's lax security and entering its partners' systems.

---

[12] AnnaMaria Andriotis, *et al.*, *Equifax Hack Leaves Consumers, Financial Firms Scrambling*, FOXBUSINESS.COM (Sept. 8, 2017), http://www.foxbusiness.com/features/2017/09/08/equifax-hack-leaves-consumers-financial-firms-scrambling.html.

[13] Michael Riley, *et al.*, *Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed*, BLOOMBERG.COM (Sept. 18, 2017), https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed?cmpid=socialflow-twitter-business&utm_content=business&utm_campaign=socialflow-organic&utm_source=twitter&utm_medium=social.

38. Equifax estimates that 145.5 million Americans were impacted by this breach.[14] It has not speculated on the number of financial institutions put at risk by this breach, and has only admitted to losing Payment Card Data for roughly 200,000 payment cards. However, card brand alerts that inform card issuers, such as FI Plaintiffs, have started rolling in. These alerts already have revised the supposed beginning date of the breach from July 2017 all the way back to November 2016.

39. Equifax reportedly discovered this breach on July 29, 2017.[15]

40. After Equifax discovered the breach, but before Equifax disclosed it to the public, three high-level executives sold shares in the company worth nearly $1.8 million.[16] On August 1, 2017 just three days after Equifax discovered the breach, Equifax Chief Financial Officer John Gamble sold $946,374 worth of stock, and President of U.S. Information Solutions Joseph Loughran exercised options to sell

---

14 Hamza Shaban, *Equifax says 2.5 million more may have been swept up in massive data breach*, WASHINGTON POST (Oct. 2, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/02/equifax-says-2-5-million-more-may-have-been-swept-up-in-massive-data-breach/?utm_term=.f1f77ea141dd.

15 *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* note 6.

16 Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, BLOOMBERG.COM (Sept. 7, 2017), https://www.bloomberg.com/news/articles/2017-09-07/three-equifaxexecutives-sold-stock-before-revealing-cyber-hack.

$584,099 worth of stock. The next day, President of Workforce Solutions Rodolfo Ploder sold $250,458 worth of stock.

41. Equifax stated that on August 2, 2017, it hired the services of Mandiant, a cybersecurity firm, to internally investigate the breach.[17]

42. Equifax did not report this breach to the public until September 7, 2017. To date, Equifax has not explained its delay in reporting this breach to the public.

43. After the breach was publicly revealed, Equifax created a website, www.equifaxsecurity2017.com, to enable consumers to check whether they were potentially impacted by the data breach. Once a consumer disclosed additional highly sensitive information to Equifax, namely their last name and last six digits of their social security number, Equifax would inform the consumer whether they had been impacted by the breach.

44. On the same page that informed the consumer whether they had been impacted or not, Equifax also directed consumers to a free identity theft protection and credit monitoring program, TrustedID,[18] they were offering in the wake of the breach. By signing up for TrustedID, consumers consented to settle all claims arising

---

[17] *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* note 6.

[18] TrustedID is a wholly owned subsidiary of Equifax, whose data breach is the basis for this complaint.

out of the use of TrustedID in arbitration, but retained their rights to trial of claims arising out of the data breach.

45. Starting on September 9, 2017, and commensurate with its ineptitude regarding data security, Equifax erroneously directed consumers to a spoof website at least four times via Twitter.[19] Rather than directing consumers to www.equifaxsecurity2017.com to determine whether consumer sensitive information was potentially compromised, Equifax mistakenly directed its Twitter followers to www.securityequifax2017.com, a website that was created by swapping the two words around and whose sole purpose was to highlight the vulnerabilities of the website Equifax created to assist potential victims.

46. Federal regulators announced they were investigating Equifax's delayed notification about the breach. The FBI is also investigating the breach, and two congressional committees announced that they would hold hearings.[20]

47. On September 13, 2017, Visa issued a CAMS alert stating that it had been notified by an acquirer of a potential network intrusion at Equifax that has put

---

19 Janet Burns, *Equifax Was Linking Potential Breach Victims On Twitter To A Scam Site*, FORBES.COM (Sept. 21, 2017), https://www.forbes.com/sites/janetwburns/2017/09/21/equifax-was-linking-potential-breach-victims-on-twitter-to-a-scam-site/#bb68b87288f2.

20 Andriotis, *supra* note 12.

Visa accounts at risk. The Visa CAMS alert indicated that the exposure window was approximately May 11, 2017 through July 26, 2017 and that the debit and credit card data that had been compromised included PAN, CVV2, expiration dates, and cardholder names. Visa further stated that financial institutions that received this CAMS alert should take necessary steps to prevent fraud and safeguard cardholders.

48. On September 15, 2017, Equifax announced the retirements of its Chief Information Officer and Chief Security Officer in connection with the breach and its aftermath.[21]

49. Numerous states and state attorneys general have rebuked Equifax in the wake of the breach. On September 18, 2017, New York Governor Andrew Cuomo directed the state's Department of Financial Services to develop a rule forcing credit reporting agencies to register with the state and comply with its cybersecurity requirements.[22] On September 19, 2017 attorneys general from 43 states and the District of Columbia signed a letter to Equifax, criticizing Equifax for

---

21 *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* note 6.

22 Ashley Southall, *Cuomo Proposes Stricter Regulations for Credit Reporting Agencies*, NEW YORK TIMES (Sept. 18, 2017), https://www.nytimes.com/2017/09/18/nyregion/equifax-hack-credit-reporting-agencies-regulations.html.

the data breach and its response.[23] The same day, Massachusetts Attorney General Maura Healey filed a suit against Equifax, seeking financial penalties and disgorgement of profits, alleging that the Company failed to promptly notify the public of the breach, failed to protect the personal data in its possession, and engaged in unfair and deceptive trade practices.[24]

50. On September 26, 2017, Equifax announced the abrupt retirement of its CEO, Richard Smith, less than three weeks after Equifax disclosed the data breach to the public and amid intense criticism of the Company.[25]

51. On October 2, 2017, Equifax announced that Mandiant had completed its internal forensic analysis of the data breach. Mandiant determined that an

---

23 Jack Suntrup, *Hawley, Madigan criticize Equifax in letter signed by other state attorneys general*, ST. LOUIS POST-DISPATCH (Sept. 19, 2017), http://www.stltoday.com/business/national-and-international/hawley-madigan-criticize-equifax-in-letter-signed-by-other-state/article_868a0dbf-1ec6-57e0-87a7-6d008005f8f0.html.

24 David Lynch, *Equifax faces legal onslaught from US states*, FINANCIAL TIMES (Sept. 21, 2017), https://www.ft.com/content/bf04768c-9e1b-11e7-8cd4-932067fbf946.

25 Hamza Shaban, *Equifax CEO Richard Smith steps down amid hacking scandal*, WASHINGTON POST (Sept. 26, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/26/equifax-ceo-retires-following-massive-data-breach/?utm_term=.995964f8571c.

additional 2.5 million consumer records may have been compromised, bringing the total number of potentially compromised accounts to 145.5 million.[26]

52. Upon information and belief, although many weeks have passed since Equifax discovered the breach, the investigation is still ongoing, and the identity of the hackers is still unknown.

53. This breach is one of the largest data breaches in history, measured by both the sheer number of people exposed and the sensitivity of the information compromised: "[t]he Equifax hack is potentially the most dangerous of all, though, because the attackers were able to gain vast quantities of PII— names, addresses, Social Security numbers and dates of birth—at one time."[27]

The Breach Was the Result of Equifax's Active Mishandling of Consumer Data and Failure to Properly and Adequately Secure Its Systems

54. The Equifax Data Breach was the direct result of Equifax's active mishandling of its IT systems and failure to properly and adequately secure its systems, which contained PII and Payment Card Data.

55. Specifically, Equifax, in making affirmative decisions with regard to its active management of its IT systems, ingored warnings from security experts about

---

26 Hamza Shaban, *supra* note 14.

27 Andriotis, *supra* note 12.

the vulnerabilities in its Apache Strut software. Additionally, Equifax failed to update this software to its latest version. In a statement posted September 14, 2017, The Apache Software Foundation attributed the Equifax Data Breach to Equifax's "failure to install the security updates provided in a timely manner."[28]

56. Equifax admitted in public statements that hackers were able to access this data by exploiting a vulnerability in Equifax's U.S. website application to illegally gain access to consumer files.

57. Equifax should have recognized and identified the flaws in its data security and should have taken measures to fix these vulnerabilities. Given the fact the only product Equifax sells is highly sought-after data of the highest sensitivity, Equifax had a duty to employ up-to-the-minute data security and to use industry best practices to prevent a security breach.

58. Even before this incident, Equifax was on notice of potential problems with its web security. A security researcher has reported that in August, hackers claimed to have illegally obtained credit card information from Equifax, which they

---

[28] *Id.*; The Apache Software Foundation, *MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache Struts Exploit* (Sept. 14, 2017), https://blogs.apache.org/foundation/entry/media-alert-the-apache-software.

were attempting to sell in an online database.[29] Equifax had a duty to respond to such a report of a significant software security flaw. Despite Equifax's knowledge of these potential security threats, Equifax willfully (or at least negligently) chose not to enact appropriate measures to ensure the security of its consumer files, including failing to encrypt sensitive personal and financial consumer information.

59. Specifically, as Equifax's CEO admitted, Equifax did not reduce the scope of sensitive data retained in backend databases and did not maintain adequate: vulnerability scanning and patch management processes and procedures; restrictions and controls for accessing critical databases; network segmentation between internet facing systems and backend databases and data stores; firewalls; file integrity monitoring; network, application, database, and system-level logging to monitor the network for unusual activity; and endpoint detection software to prevent exfiltration of data.[30]

60. The harm to Plaintiffs resulting from Equifax's failure to adequately secure its computer systems and websites was at all times entirely foreseeable to Equifax.

---

29 Andriotis, *supra* note 12; *see also* Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES.COM (Sept. 8, 2017), https://www.forbes.com /sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#6b43b0ea677c.

30 Smith Testimony, *supra* note 1.

61. Equifax is well aware of the costs and risks associated with payment card fraud and identity theft, and is particularly aware that FI Plaintiffs and the Class bear the ultimate responsibility for payment card fraud and identity theft, as well as the obligation to protect against it. On its website, Equifax lists "some of the ways identity theft might happen," including when identity thieves "steal electronic records through a data breach."[31]

62. Because Equifax is aware of the harm caused by payment card fraud and identity theft, Equifax itself offers products aimed at protecting consumers from such illegal activity. For example, Equifax advertises its "Equifax Complete™ Premier Plan" as "Our Most Comprehensive Credit Monitoring and Identity Protection Product."[32] The product promises to monitor consumers' credit scores, provide text message alerts when suspicious activity on consumer banking or credit card accounts occur, lock the consumer's credit file for unapproved third parties, and automatically scan suspicious websites for consumers' personal information.

---

31 Equifax, *How Does Identity Theft Happen?* https://www.equifax.com/personal/education/identity-theft/how-doesidentity-theft-happen (last accessed Oct. 3, 2017).

32 Equifax, *Equifax Complete™ Premier Plan: Our Most Comprehensive Credit Monitoring and Identity Protection Product*, https://www.equifax.com/personal/products/credit/monitoring-and-reports (last accessed Oct. 3, 2017).

63. Equifax was aware of the risk posed by its insecure and vulnerable website. It was also aware of the extraordinarily sensitive nature of the personal information that it maintains as well as the resulting impact that a breach would have on consumers and financial institutions – including FI Plaintiffs and the other class members.

Equifax Violated Federal Security Requirements and Other Industry Standards

64. The Equifax breach is unique because safeguarding FI Plaintiffs' and consumer's highly sensitive personal information is one of the few responsibilities the company has, since sensitive data is the only product in which the company trades. As a company that deals exclusively in sensitive data, Equifax has a clear legal duty to maintain the confidentiality of FI Plaintiffs' and consumer's sensitive information and prevent any third-party misuse or access to such information. Equifax's utter failure to safeguard consumer information violates federal data security standards and industry standards, as well as a clearly established legal duty to not act negligently when handling and storing PII and Payment Card Data.

Equifax Failed to Comply with Federal Trade Commission Requirements

65. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data

constitutes an unfair act or practice prohibited by Section 5 of the FTC Act of 1914 ("FTC Act"), 15 U.S.C. §45.

66. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

67. The FTC also has published a document entitled "FTC Facts for Business" which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

68. And the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

69. In the months and years leading up to the data breach and during the course of the breach itself, Equifax did not follow the guidelines recommended by the FTC. Further, by actively mishandling the security of its IT systems and failing to have reasonable data security measures in place, Equifax engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

Equifax Failed to Comply with Industry Standards for Data Security

70. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit Payment Card Data. These standards, known as the Payment Card Industry Data Security Standard ("PCI DSS"), are the industry standard governing the security of Payment Card Data. It sets the minimum level of what must be done, not the maximum.

71. PCI DSS 3.2, the version of the standards in effect beginning in April 2016, impose the following 12 "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Furthermore, PCI DSS 3.2 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates.

72. Among other things, PCI DSS required Equifax to properly secure Payment Card Data; not store cardholder data beyond the time necessary to authorize a transaction; implement proper network segmentation; encrypt Payment Card Information at the point-of-sale; restrict access to Payment Card Information to those with a need to know; and establish a process to identify and timely fix security vulnerabilities. As discussed herein, Equifax failed to comply with each of these requirements.

FI Plaintiffs Have Been, Are Currently Being, and Will Be Harmed by the Equifax Data Breach

73. The Equifax Data Breach has inflicted immediate, hard costs on FI Plaintiffs and members of the class similar to other data breaches in which Payment

Card Information is stolen. This includes costs for payment card cancellation and replacement, coverage of fraud charges on affected accounts, costs of notifying customers, opening and closing affected accounts, lost interchange fees, and other damages.

74. Unlike other data breaches, however, the Equifax Data Breach has caused severe, long term damages in myriad other ways. Because Equifax provides services that are so core to the business functioning of credit extenders and lenders such as Plaintiff and members of the proposed class, the true extent of the damage may take years to fully materialize. Immediately, however, FI Plaintiffs and members of the proposed class are faced with the costs of dealing with customers who freeze their credit, making it impossible to determine their creditworthiness for current or potential credit or loans or to comply with regulatory requirements. FI Plaintiffs and the Class are also faced with the requirement that in order to carry out their business functions, they must exchange the most sensitive customer information to a company that has proven to have no ability to secure data.

75. Furthermore, and perhaps most significantly, FI Plaintiffs and the Class also face the obligation to pay for the costs of identity theft and fraudulent credit and other accounts for which the consumer victims are not responsible. The certain impending risk of identity theft and loan fraud as a direct result of the Equifax

breach, and the protections which must be now put in place to limit such risks, represents significant harm to Plaintiffs.

76. Equifax actively mishandled its data security and IT systems and chose not to follow industry standards and failed to effectively monitor its security systems to ensure the safety of customer information. Equifax's substandard security protocols and failure to adequately monitor for unauthorized intrusion caused consumers' PII and Payment Card Data to be compromised for months without detection by Equifax.

77. Furthermore, FI Plaintiffs' own data security is now at an increased and certain impending risk of being breached due to hackers accessing Equifax's back-end servers that are connected to FI Plaintiffs' servers. This intrusion has left FI Plaintiffs exposed to the threat of hackers piggybacking off of Equifax's insufficient security to attack those who do business with Equifax.

78. FI Plaintiffs have incurred and will continue to incur substantial damage because of Equifax's failures to meet reasonable standards of data security. FI Plaintiffs have had to immediately react to mitigate the fraudulent transactions being made on payment cards they had issued while simultaneously taking steps to prevent future fraud, including identity theft which will lead to loan fraud. FI Plaintiffs are also in a heightened state of alert and are incurring significant

administrative costs regarding their own data security as a result of the hackers' potential access to their networks via the digital connection shared with Equifax.

79. As a result of the Equifax data breach, FI Plaintiffs and the Class are required to cancel and reissue payment cards, change or close accounts, notify customers that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on their own networks as well as on potentially impacted accounts, go to greater lengths to verify the identity of consumers seeking loans in light of impending credit freezes, and take other steps to protect themselves and their customers, in an effort to reduce the risk of future, but certainly impending, identity theft, loan fraud, and other fraudulent consumer transactions.

80. FI Plaintiffs and the Class also lost interest revenue and transaction fees due to reduced payment card usage. Furthermore, debit and credit cards belonging to FI Plaintiffs and the Class, as well as the account numbers on the face of the cards, were devalued. This devaluation of the payment cards and the data set forth on them represents real, quantifiable damage to the property of FI Plaintiffs and the Class.

81. Sensitive personal and financial information, like the information compromised in this breach, is extremely valuable to thieves and hackers. These criminals have gained access to complete profiles of individuals' personal and

financial information. They can now use this data to steal the identities of the consumers whose information has been compromised or sell it to others who plan to do so. The identity thieves can assume these consumers' identities (or create entirely new identities from scratch) to make transactions or purchases, open credit or bank accounts, apply for loans, forge checks, commit immigration fraud, obtain a driver's license in the member's or customer's name, obtain government benefits, or file a fraudulent tax return. A report by the Department of Justice found that 86% of identity theft victims in 2014 experienced the fraudulent use of existing account information, including credit card and bank account information.[33]

82. While consumers are ultimately protected from most fraud loss arising from this incident, FI Plaintiffs and the Class are not, as they bear the primary responsibility for reimbursing customers for fraudulent charges, fraudulently opened accounts, and covering the costs of issuing new payment cards for customers to use and implementing new customer security and authentication procedures. Additionally, FI Plaintiffs and the Class will suffer financial losses whenever an identity is stolen and used to falsely establish credit, create a deposit account, or access an existing customer's account. This certainly impending risk will continue

[33] Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS, NCJ 248991 (Sept. 2015) at 1, https://www.bjs.gov/content/pub/pdf/vit14.pdf.

into the foreseeable future, and will require FI Plaintiffs and the Class to incur significant costs and expenses in order to reduce and mitigate it.

83. Financial institutions are responsible for all charges to fraudulently opened accounts. When complete consumer profiles have been compromised, financial institutions experience continuous losses as identity thieves move on from one consumer profile to the next. With a breach of this magnitude, there is virtually no limit to the amount of fraudulent account openings financial institutions may face. These risks are very real in the wake of the Equifax breach and are certainly impending.

84. As a result of the Equifax data breach, financial institutions face considerable costs associated with monitoring, preventing, and responding to fraudulent charges and account openings. Financial institutions must implement additional fraud monitoring and protection measures, institute new customer security and authentication procedures, investigate potentially fraudulent activity, and indemnify members or customers for fraudulent charges. Financial institutions will also need to take other necessary steps to protect themselves and their members or customers, including notifying members or customers, as appropriate, that their accounts may have been compromised.

85. Consumers inevitably face significant emotional distress after theft of their identity. The fear of financial harm can cause significant stress and anxiety for many consumers. According to the Department of Justice, an estimated 36% of identity theft victims experienced moderate or severe emotional distress as a result of the crime.[34] This stress also impacts financial institutions, which are forced to expend additional customer service resources helping their concerned customers. Customers experiencing severe anxiety related to identity theft are often hesitant to use some banking services altogether, instead opting to use cash. As a result, financial institutions forgo many of the transaction fees, ATM fees, interest, or other charges that they may have otherwise collected on these accounts.

86. In addition, financial institutions have and will continue to incur significant costs in implementing additional customer authentication methods, such as, for example, multi-factor customer authentication. These measures are necessary as a direct and mitigating response to the Equifax data breach.

87. Financial institutions will also face increased regulatory compliance costs going forward as a result of this incident. Federal regulators have already begun considering the implications of the breach and are likely to implement additional requirements to protect consumers from the financial risks associated with this

34 *Id.*

breach. For example, additional reports and plans will likely be required to satisfy regulators. Financial institutions will be required to directly bear the administrative costs of these additional measures.

88. Financial institutions are also harmed by the chilling effect this breach will have on future lending as consumers deal with the impact of the breach on their finances and credit. Customers or members are often without access to their accounts for several days at a time while credit or debit cards are replaced or accounts are changed. Additionally, some customers are hesitant to use card transactions altogether in the wake of a major breach. This results in lost fees and interest to the financial institutions issuing these cards.

89. Financial institutions are also harmed by the chilling effect this breach will have on consumers willingness to seek extensions of credit through instruments like home mortgages and credit cards. Customers who do not react to the breach by placing a freeze on their credit, may nevertheless refrain from obtaining credit in the wake of the breach. This results in lost fees and interest to financial institutions.

90. Moreover, Equifax's massive and destabilizing data breach threatens to severely disrupt the usual business operations of nearly every bank and credit union in the nation. This is because banks and credit unions rely upon Equifax to provide services that are core to the institutions' credit extension, lending, and other

functions. The inability to reliably exchange the information that underlies these functions inflicts great, and real, risk and uncertainty to the financial institution's business models.

91. As a result of the breach, financial institutions have incurred significant costs in notifying their customers and responding to inquiries from customers about the breach.

92. Even more worrisome, financial institutions are often required to demonstrate the health of their credit and loan portfolios to regulators, who require credit reports be pulled to analyze the strength of the portfolio. Such regulatory requirements cannot be met where great portions of consumers have implemented credit freezes, which are cumbersome and costly to switch on and off.

93. Ultimately, Plaintiffs and the Class are faced with considerable present injury, and an immediate future of continually unfolding new and continued injuries as a result of Equifax's avoidable data breach.

Equifax Had a Clear Legal Duty to Prevent and Timely Report this Breach

94. Equifax had a legal duty – owed to the financial institutions which bear the readily foreseeable risk of injury – to prevent a breach of consumers' sensitive personal information.

95. Following several high-profile data breaches in recent years, including Target, Experian, Yahoo, Home Depot, and Sony, Equifax was on notice of the very real risk that hackers could exploit vulnerabilities in its data security. Moreover, Equifax has considerable resources to devote to ensuring adequate data security.

96. Nonetheless, Equifax failed to invest in adequate cyber security measures to properly secure its U.S. website from the threat of hackers.

97. Financial institutions were harmed not only by the breach itself, but also by Equifax's failure to timely report this breach to the public.

98. Equifax discovered this breach on July 29, 2017, but did not report it to the public until nearly six weeks later, on September 7, 2017.

99. According to one report, an anonymous source familiar with the investigation states that "Equifax executives decided to hold off on informing the public until they had more clarity on the number of people affected and the types of information that were compromised."[35] But Equifax has not yet given an official explanation for its delay in reporting this breach to the public. In the time between when Equifax discovered this breach and when it reported the breach to the public, however, three of its top executives sold substantial sums of stock in the company,

---

35 *Id.*

presumably avoiding the financial losses associated with the negative press Equifax has received since the breach.[36]

100. Because of this delay, consumers with compromised personal information and credit card information have been unable to adequately protect themselves from potential identity theft for several weeks. The consequences to financial institutions from this delay are very real, given that they ultimately bear financial responsibility for the fraud inflicted upon consumers.

101. Financial institutions have been unable to alert their members or customers of the risk in a timely manner, or to implement measures to detect and prevent potential fraud in the time before the breach was disclosed. The failure of Equifax to report the breach in a timely manner has resulted in additional harm to FI Plaintiffs and the Class.

Equifax Has a History of Poor Data Security

102. Even before the 2017 data breach, Equifax was on notice of potential problems with its web security and has suffered from multiple security breaches in the past.

---

[36] Equifax's stock prices dropped almost 15% the day after the breach was publicly announced—the largest decline in nearly two decades. Ben Eisen, *Equifax Shares on Pace for Worst Day in 18 Years*, WALL STREET JOURNAL (Sept. 8, 2017), https://blogs.wsj.com/moneybeat/2017/09/08/equifaxshares-on-pace-for-worst-day-in-18-years/.

103. In April of 2016, it was revealed that hackers were able to exploit Equifax's W-2Express website, an Equifax service for companies to make electronic W-2 forms accessible to employees, and accessed employees' sensitive tax data. Through an online portal, the hackers only had to enter an employee's default PIN code, which was simply the last four digits of the employee's Social Security number, and the employee's four-digit birth year. More than 400,000 employees' W-2 tax information was subsequently left open to theft.[37]

104. The use of simple and easily identifiable information for a default login and password to access sensitive personal and financial data is a substandard security practice. Indeed, shortly after Equifax publicly announced the breach at issue, security researchers discovered that one of Equifax's online employee portals could be accessed by using the word "admin" for both the login and password. Once logged in through the portal, a user could easily access sensitive employee and consumer data.[38]

---

37 *See* Brian Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY, May 16, 2016, https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/.

38 *See* Brian Krebs, *Auyda Help Equifax Has My Data*, KREBS ON SECURITY (Sept. 17, 2017), https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/.

105. Security researchers have also questioned for years Equifax's use of an easily identifiable security PIN issued to consumers who have requested to lock their credit report. When a consumer requests a credit lock, Equifax provides a security PIN that the consumer can then later use to unlock their credit. Instead of providing a secure, randomized PIN, Equifax only issues a date-time stamp of when the consumer requested the lock. Such an easily discernible PIN vastly increases the odds of someone attempting to unlock a credit report for the purposes of identity theft. Equifax has recently stated they are now taking steps to provide randomly generated PINs.[39]

106. The impact of such weak security practices often results in the exploitation of consumer information in the black market. As one security researcher reported, hackers claimed to have illegally obtained credit card information from Equifax, which they were attempting to sell in an online database.[40]

CLASS ACTION ALLEGATIONS

---

[39] *See* Sean Gallagher, *Equifax Moves To Fix Weak PINs For 'Security Freez' On Consumer Credit Reports*, ARSTECHNICA (Sept. 11, 2017), https://arstechnica.com/information-technology/2017/09/equifax-moves-to-fix-weak-pins-for-security-freeze-on-consumer-credit-reports/.

[40] Andriotis, *supra* note 12; *see also* Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES (Sept. 8, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-databreach-history/#63dc4270677c.

107. FI Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of the following class:

> **FI Plaintiffs Nationwide Class**: All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) who issue payment cards and/or otherwise extend credit to consumers whose data was exposed between May 2017 and July 2017 as a result of the Equifax Data Breach.

Rule 23(a)

108. This action may properly be maintained as a class action and satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

109. **Numerosity**. The members of the Class are so numerous that joinder would be impracticable. FI Plaintiffs believe the number of Class members exceeds 10,000.

110. **Commonality**. There are common questions of law and fact that predominate over questions affecting only individual Class members. These common legal and factual questions include, but are not limited to:

a. whether Equifax owed a duty to FI Plaintiffs and members of the Class to protect PII and Payment Card Data;

b. whether Equifax failed to provide reasonable security to protect PII and Payment Card Data;

c. whether Equifax negligently or otherwise improperly allowed PII and Payment Card Data to be accessed by third parties;

d. whether Equifax failed to adequately notify FI Plaintiffs and members of the Class that its data systems were breached;

e. whether FI Plaintiffs and members of the Class were injured and suffered damages and ascertainable losses;

f. whether Equifax's failure to provide reasonable security proximately caused the injuries suffered by FI Plaintiffs and members of the Class;

g. whether FI Plaintiffs and members of the Class are entitled to damages and, if so, the measure of such damages; and

h. whether Plaintiffs and members of the Class are entitled to declaratory and injunctive relief.

111. **Typicality.** FI Plaintiffs' claims are typical of the claims of the absent class members and have a common origin and basis. FI Plaintiffs and absent Class members are all financial institutions injured by Equifax's data breach. The FI Plaintiffs' claims arise from the same practices and course of conduct giving rise to

the claims of the absent Class members and are based on the same legal theories, namely the Equifax data breach. If prosecuted individually, the claims of each Class member would necessarily rely upon the same material facts and legal theories and seek the same relief. FI Plaintiffs' claims arise from the same practices and course of conduct that give rise to the other Class members' claims and are based on the same legal theories.

112. **Adequacy**. FI Plaintiffs will fully and adequately assert and protect the interests of the absent Class members and have retained Class counsel who are experienced and qualified in prosecuting class action cases similar to this one. Neither FI Plaintiffs nor their attorneys have any interests contrary to or conflicting with the interests of absent class members.

Rule 23(b)(3)

113. The questions of law and fact common to all Class members predominate over any questions affecting only individual class members.

114. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class members' claims is economically infeasible and procedurally impracticable. Class members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and will prevent

delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class members to litigate their claims where it would otherwise be too expensive or inefficient to do so. FI Plaintiffs know of no difficulties in managing this action that would preclude its maintenance as a class action.

Rule 23(b)(2)

115. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

116. Contact information for each Class member, including mailing addresses, is readily available, facilitating notice of the pendency of this action.

COUNT I
Negligence
(On behalf of FI Plaintiffs)

117. FI Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

118. Equifax owed – and continues to owe – a duty to FI Plaintiffs and members of the Class, to use reasonable care in safeguarding PII and Payment Card Data and to notify them of any breach in a timely manner so that appropriate action

can be taken to minimize or avoid losses. This duty arises from several sources, including, but not limited to, the sources described below, and is independent of any duty Equifax owed as a result of any of its contractual obligations.

119. Equifax has a common law duty to prevent the foreseeable risk of harm to others, including FI Plaintiffs and the Class. The duty to protect others against the risk of foreseeable criminal conduct has been recognized in situations in which the parties are in a special relationship, or where an actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk. See Restatement (Second) of Torts, §302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard PII, Payment Card Data, and other sensitive information.

120. It was foreseeable that injury would result from Equifax's failure to use reasonable measures to protect PII and Payment Card Data and to provide timely notice of a breach. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal PII and/or Payment Card Data belonging to millions of consumers; thieves would use the PII and Payment Card Data to create the injury and damages described herein.

121. There is no question that the prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and

growing economic drain on individuals, businesses, and government entities in the United States. According to the Identity Theft Resource Center, the year 2016 saw a total of 1,093 reported data breaches in the United States, an all-time high.[41] More than 36 million records were reportedly exposed in those breaches.[42]

122. It is well known that a common motivation of data breach perpetrators is the hackers' intentions to sell PII and/or Payment Card Data on underground black markets, and news outlets reported that this, in fact, occurred after the Home Depot and Target data breaches, among others. Malicious or criminal attacks were the cause of 50% of the breaches covered by the IBM study, and were also the most costly.[43]

123. In tandem with the increase in data breaches, the rate of identity theft also reached record levels in 2016, affecting approximately 15.4 million victims in the United States and resulting in approximately $16 billion worth of fraud losses.[44]

---

41 Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html.

42 Identity Theft Resource Center, *Data Breach Reports: 2016 End of Year Report (*Jan. 18, 2017), at 226, http://www.idtheftcenter.org/images/breach /2016/DataBreachReport_2016.pdf.

43 *Id.* at 8.

44 Javelin Strategy & Research, *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy &*

In this environment, every reasonable person and company in the United States is aware of the significant risk of criminal attacks against computer systems that store PII, Payment Card Data and other sensitive information.

124. Equifax assumed the duty to use reasonable security measures as a result of its conduct, internal policies and procedures, and Privacy Policy in which the company stated it was using "industry standard means" of protecting PII and Payment Card Data, and that its security measures were "appropriate for the type of information we collect." By means of these statements, Equifax specifically assumed the duty to comply with industry standards, including PCI DSS and every other conceivable standard applicable to a company whose sole business is transacting in the most sensitive consumer information there is.

125. A duty to use reasonable security measures also arises as a result of the special relationship that existed between Equifax and FI Plaintiffs and the Class. The special relationship arises because financial institutions entrusted Equifax with customer PII and Payment Card Data. Only Equifax was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

Research Study (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.

126. Equifax's duty to use reasonable data security measures also arises under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by retailers such as Equifax. FTC publications and data security breach orders further form the basis of Equifax's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

127. Equifax's duty to use reasonable care in protecting PII and Payment Card Data arises not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

128. Equifax breached its common law, statutory and other duties – and was negligent – by failing to use reasonable measures to protect consumers' personal and financial information from the hackers who perpetrated the data breach and by failing to provide timely notice of the breach. The specific negligent acts and omissions committed by Equifax include, but are not limited to, the following:

a. failure to employ reasonable systems to protect against malware;

b. failure to regularly and reasonably update its antivirus software;

c. failure to maintain an adequate firewall;

d. failure to reasonably track and monitor access to its network and consumer data;

e. failure to reasonably limit access to those with a valid purpose;

f. failure to heed warnings about specific vulnerabilities in its systems identified by Equifax's own employees, consultants, and software vendors;

g. failure to recognize red flags signaling that Equifax's systems were inadequate and that, as a result, the potential for a massive data breach akin to the one involving Target and Home Depot was increasingly likely;

h. failure to recognize that hackers were stealing PII and Payment Card Data from its systems while the data breach was taking place; and

i. failure to disclose the data breach in a timely manner.

129. As a direct and proximate result of Equifax's negligence, FI Plaintiffs and the Class have suffered and continue to suffer injury as described herein.

130. Because no statutes of other states are implicated, Georgia common law applies to the negligence claims of FI Plaintiffs and the Class.

COUNT II
Negligence Per Se
(On behalf of FI Plaintiffs)

131. FI Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

132. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by consumer-serving organizations such as Equifax of failing to use reasonable measures to protect PII and Payment Card Data. The FTC publications and orders described above also form the basis of Equifax's duty.

133. Equifax violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and Payment Card Data and by not complying with applicable industry standards, including PCI DSS. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach at a major credit reporting agency, including specifically the immense damages that would result to consumers and financial institutions.

134. Equifax's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

135. FI Plaintiffs and the Class are within the scope of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for paying for and reimbursing consumers for fraud losses. Moreover, many of the class members are credit unions, which are organized as cooperatives whose members are consumers.

136. Furthermore, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by FI Plaintiffs and the Class here.

137. As a direct and proximate result of Equifax's negligence per se, FI Plaintiffs and the Class have suffered and continue to suffer injury and damages as described herein.

138. Because no statutes of other states are implicated, Georgia common law applies to the negligence per se claim of FI Plaintiffs and the Class.

COUNT III
Declaratory and Equitable Relief
(On Behalf of FI Plaintiffs)

139. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

140. Under the Declaratory Judgment Act, 28 U.S.C. §2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and that violate the terms of the federal and state statutes described in this complaint.

141. An actual controversy has arisen in the wake of Equifax's data breach regarding its common law and other duties to reasonably safeguard its customers' PII and Payment Card Data. Plaintiffs allege that Equifax's data security measures were inadequate and remain inadequate. Furthermore, Plaintiffs continue to suffer injury and damages as described herein.

142. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Equifax continues to owe a legal duty to secure PII and Payment Card Data under, *inter alia*, the common law and Section 5 of the FTC Act;

b. Equifax continues to breach its legal duty by failing to employ reasonable measures to secure PII and Payment Card Data; and

c. Equifax's ongoing breaches of its legal duty continue to cause Plaintiffs harm.

143. The Court should also issue corresponding injunctive relief requiring Equifax to employ adequate security protocols consistent with industry standards to protect PII and Payment Card Data. Specifically, this injunction should, among other things, direct Equifax to:

a. implement encryption keys in accordance with industry standards;

b. consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;

c. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

d. regularly test its systems for security vulnerabilities, consistent with industry standards; and

e. install all upgrades recommended by manufacturers of security software and firewalls used by Equifax.

144. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Equifax, which is a real possibility given the continued missteps taken by Equifax described herein, including using its official corporate communications to send affected consumers to

phishing sites. Indeed, Equifax was hit with a separate data breach in March 2017 that apparently did nothing to motivate the company to discover the other massive data breach going on at the same time.[45] The risk of another such breach is real, immediate, and substantial. If another breach at Equifax occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

145. The hardship to FI Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Equifax if an injunction is issued. Among other things, if another massive data breach occurs at Equifax, FI Plaintiffs and the Class will likely incur millions of dollars in damages. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security measures is relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

146. Issuance of the requested injunction will serve the public interest by preventing another data breach at Equifax, thus eliminating the injuries that would

[45] Mark Coppock, *Equifax Confirms It Suffered A Separate Data Breach In March*, DIGITAL TRENDS (Oct. 3, 2017), https://www.digitaltrends.com /computing/equifax-data-breach-affects-143-million-americans/.

result to Plaintiffs, the Class, and the potentially millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, FI Plaintiffs, individually and on behalf of the Class, respectfully request that the Court:

a. Certify the Class and appoint FI Plaintiffs and FI Plaintiffs' counsel to represent the Class;

b. Enter a monetary judgment in favor of FI Plaintiffs and the Class to compensate them for the injuries they have suffered and will continue to suffer, together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

c. Enter a declaratory judgment as described herein and corresponding injunctive relief requiring Equifax to employ adequate security protocols consistent with industry standards to protect PII and Payment Card Data;

d. Grant the injunctive relief requested herein;

e. Award FI Plaintiffs and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and

f. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all claims so triable.

Respectfully submitted this 5th day of January, 2018,

By: */s/ Thomas A. Withers*
Thomas A. Withers
Ga. Bar No. 772250
GILLEN WITHERS & LAKE, LLC
8 E. Liberty Street
Savannah, GA 31401
Telephone: 912.447.8400
Facsimile: 912.629-6347
twithers@gwllawfirm.com

Anthony C. Lake
Ga. Bar No. 431149
GILLEN WITHERS & LAKE, LLC
3490 Piedmont Road, N.E.
One Securities Centre, Suite 1050
Atlanta, GA 30305
Telephone: 404.842.9700
Facsimile: 404.842.9750
aclake@gwllawfirm.com

Joseph P. Guglielmo
Erin Green Comite
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212.223.6444
Facsimile: 212.223.6334
jguglielmo@scott-scott.com
ecomite@ scott-scott.com

Gary F. Lynch
Jamisen A. Etzel
Bryan A. Fox
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
glynch@carlsonlynch.com
jetzel@carlsonlynch.com
bfox@carlsonlynch.com

Karen Hanson Riebel
Kate M. Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612-339-0981)
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Bryan L. Bleichner
CHESTNUT CAMBRONNE
17 Washington Avenue North
Suite 300
Minneapolis, MN 55401
Telephone: 612.339.7300
Facsimile: 612.336-2940
bbleichner@chestnutcambronne.com

Arthur M. Murray
Stephen B. Murray, Sr.
Caroline W. Thomas
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Telephone: 504.525.8100
Facsimile: 504.584.5249
amurray@murray-lawfirm.com
smurray@murray-lawfirm.com
cthomas@murray-lawfirm.com

Brian C. Gudmundson
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: 612.341.0400
Facsimile: 612.341.0844
brian.gudmundson@zimmreed.com

Charles H. Van Horn
BERMAN FINK VANHORN P.C.
3475 Piedmont Road, Suite 1100
Atlanta, GA 30305
Telephone: 404-261-7711
Facsimilie: 404-233-1943
cvanhorn@bfvlaw.com

Counsel for Plaintiffs

CERTIFICATION

The undersigned hereby certifies, pursuant to Local Rule 7.1(D), that the foregoing document has been prepared with one the font and point selections (Times New Roman, 14 point) approved by the Court in Local Rule 5.1(C).

/s/ Thomas A. Withers

Thomas A. Withers
Ga. Bar No. 772250
GILLEN WITHERS & LAKE, LLC
8 E. Liberty Street
Savannah, GA 31401
Telephone: 912.447.8400
Facsimile: 912.629-6347
twithers@gwllawfirm.com